



# APPLICATIONS OF BIOMETRIC AUTHENTICATION: AN ANALYSIS AND COMPARISON

A. K. Shrivastava<sup>1</sup> | Swati Bareth<sup>1</sup>

<sup>1</sup> Dept. Of IT, Dr. C. V. Raman University, Bilaspur (C. G.), India.

## ABSTRACT

Biometrics authentication is a growing technology which has been used in huge areas like forensics, telecommunication, government, traffic and health care services. A biometric authentication system provides recognition of an each and every person based on physiological or behavioral characteristics. In this paper the main focus is an comparison of various biometric systems such as iris, retina, DNA, face, ear, voice, heartbeat, gait etc. and simply define their advantages, disadvantages, feature and application. The comparison criteria are accuracy, cost, performance, acceptability etc.

**KEY WORDS:** Biometric Authentication System, Analysis, Applications, Comparison.

## 1. INTRODUCTION

Security is one of the important issues to protect the information and information system from unauthorized persons. There are various organization, institutes and industry are facing the problem of security and using various authentication system to identify the authorized person. Authentication of users in computer system is done based on certain security measures like passwords, keys, id cards pin number etc. Biometric is very important authentic systems to identification the authorized person and protect the system from unauthorized person. Biometric authentication supports the identification, authentication and no repudiation [3]. Biometrics is a technique for recognizing the human characters. Biometric authentication is used in various areas like banking, aviation, financial transactions, forensic etc. [4].

There are various authors have work in areas of biometric authentication. S. Tiwari et al. [6] have described about advantages, limitations, principles of area and applications of all the biometric authentication system after comparing all

the existing biometric technology on the basis of various parameters. H. Srivastava [5] has described the uses of each and every biometric system and selection of particular biometric device depends upon the application area. It also compared all the biometric system on the basis of various factors like Uniqueness, Universality, Performance, Acceptability etc. B. Kaschte [7] has described about biometrics authentication their types, advantages, disadvantages and future use. A. K. Jain et al. [8] have described features, advantages and applications in forensic, civilian and in commercial field. It also compared all the existing biometric technology on the basis of various parameters. S. Singh et al. [2] have explored physical and behavioral biometric, advantages and disadvantages of all biometric systems and compare all the biometric technology depends on various criteria.

## 2. TYPES OF BIOMETRIC AUTHENTICATION SYSTEM

In this research work, we have explored various biometric authentication and its advantages, disadvantages, features and applications as shown in **Table 1**.

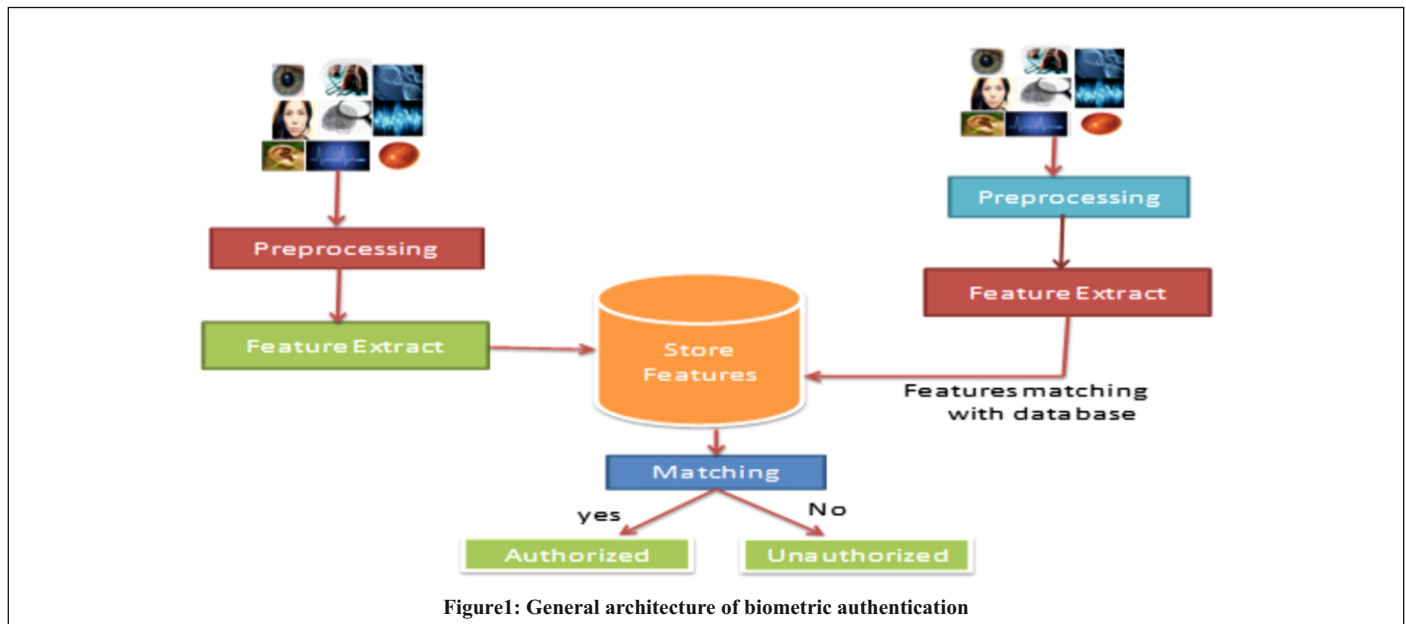
**Table1: Various biometric authentication systems**

Biometric System	Advantage	Disadvantage	Feature	Application
Face [10,11]	<ul style="list-style-type: none"> <li>Easy to use</li> <li>Low cost</li> </ul>	The same person under different lighting Condition may be seen quite different.	Fast and accurate	Aadhar card, Railway, Airport and Criminal Identification.
Iris [12,19]	Stable throughout life. Uses in Birth certificate, Aadhar card	It is most expensive.	Circular structure in the eye, responsible for controlling the diameter and size of the pupils.	Forensics, birth certificates; tracing missing or wanted persons.
Fingerprints [10,19]	Not change throughout life time.	<ul style="list-style-type: none"> <li>To wet or dry fingers do not produce bitmaps with sufficient quality.</li> <li>Cheat by using Artificial Fingerprint.</li> </ul>	Fingerprint ridges and valleys are unique and unalterable.	Education, civil service, forensics.
Retina [13,14,19]	<ul style="list-style-type: none"> <li>Very stable,</li> <li>Very high accuracy</li> </ul>	<ul style="list-style-type: none"> <li>Not very user friendly.</li> <li>High equipment cost.</li> </ul>	Based on the blood vessel pattern in the retina of the eye.	Military, nuclear facilities and laboratories.
DNA [15]	DNA biometrics technology is highly unique and the chance of two individuals having the exact same DNA profile is extremely impossible.	<ul style="list-style-type: none"> <li>Expensive method</li> <li>Easy to steal someone else's DNA.</li> </ul>	Used mostly in forensics applications for identifying people.	<ul style="list-style-type: none"> <li>Healthcare applications involving organ donors or transplants.</li> <li>Prove guilt or innocence.</li> <li>Paternity, Maternity.</li> </ul>
Heart beat [19]	<ul style="list-style-type: none"> <li>It can't be stealing.</li> <li>It can't be lost or forgot.</li> </ul>	Too costly.	Every person has unique heartbeat it is based on size and shape of heart and they use it as a password.	It is useful in medical field for health and fitness checking.
Ear [1,16]	Ear does not change during human life.	Low accuracy	It is possible to work faster and more efficiently with the images with the lower resolution.	Law enforcement, forensics.
Gait [17]	Difficult to hide, steal or fake	No model is developed with complete accuracy till now.	Each person's walking speed and style will make the waves bounce back differently.	It could be usable for covert surveillance and detection forensics.
Signature [4]	User acceptance .	Low reliability .	It is based on measuring dynamic signature features such as speed, pressure and angle.	In person identification, forensic sciences, etc.
Voice [10]	They do not require any special and expensive hardware.	Several words sound very similarly.	Easy to use and easily accepted by user.	<ul style="list-style-type: none"> <li>Solving crimes with voice recognition.</li> <li>Letting your voice protect your bank account.</li> </ul>
Keystroke [9,17,18]	It is cost effective process.	Low accuracy, No unique to each individual	It is very easy to capture data as keyboards are common and no especial equipment is necessary.	Computer and / or workstation security.

### 3. WORKING PRINCIPLE OF BIOMETRIC AUTHENTICATION

All the biometric system uses the same basic principle. It contains predefined steps as acquire sample, feature extraction, matching sample and result. Figure 1 shows that general architecture of biometric authentication system. Firstly, the biometric sample is acquired from user. The some unique features are extracted

from biometric sample of user's and it is stored in database for later comparing to authentication of users. When the users are giving input sample that matches with one of the samples stored in database. If the input sample are matched with data base samples then biometric system allows the person to access the resources otherwise deny.



### 4. ANALYSIS AND COMPARISON OF VARIOUS BIOMETRIC AUTHENTICATION SYSTEM

In this section, we have compared various biometric authentication system based on its uniqueness, universality, performance, permanence, acceptability, Circumvention and Collectability. Uniqueness is how well the biometric separates individually from another. Universality is the quality of being universal; existing everywhere, Performance means accuracy, speed, and robustness of technology

used. Permanence is the biometric should be sufficiently invariant over a certain period of time. Acceptability means to extent society is supporting. Circumvention is the act of cheating someone and Collectability is how well the identifiers can be captured and quantified. **Table 2** shows that comparison of biometric authentication system using different factors. These all are factors value like low, medium and high based on advantaged, disadvantages, features and its applications as explained below.

**Table 2: Comparison of biometric authentication system using different factors**

Biometrics	Uniqueness	Permanence	Universality	Collectability	Performance	Acceptability	Circumvention
Face	low	medium	high	high	low	high	High
Iris	high	high	high	medium	high	medium	Low
Fingerprints	high	high	medium	medium	medium	high	Medium
Retina	high	high	high	low	high	low	Low
DNA	high	high	high	low	high	high	Low
Heart beat	high	high	high	low	high	low	Low
Ear	medium	medium	high	medium	low	medium	Medium
Gait	low	low	medium	low	low	high	Medium
Signature	low	low	low	high	medium	high	High
Voice	low	low	medium	medium	low	high	High
Keystroke	low	low	low	medium	low	low	Medium

**LOW:** means is not unique, frequently change, doesn't exists everywhere, low in capture or stored, not accurate, processing speed is slow, not reliable, not easy to cheat someone, not popular in people, provide low cost, low accurate, not easy in use and not stable.

**MEDIUM:** means some time it is not unique (system does not distinguish between more than two people), after some age it must be fixed or not change, stored or capture but not very well, some time it should be accurate, processing speed is not very slow but not high, some time reliable, cheat by someone is not easy but some time it is possible, sometimes popular but not very much, less expensive in cost, sometime its result is not accurate and changeable after some period.

**HIGH:** means it is more unique, not changeable, capture and stored is very easy process, accurate and reliable, not possible to cheat by someone because everyone have unique feature, give highly accurate result, expensive, highly popular, easy in use and fully stable.

### 5. CONCLUSION

A Biometric recognition refers to automatic identification of a person based on physical (e.g. iris, face etc.) and behavioral (e.g. signature, gait etc.) characteristics. This Biometric identification system provides several advantages, features and applications and compared to other traditional methods such as ID card, pin no. , password etc. Biometric system is less expensive and miniaturized and it provides protection, privacy from fraud. In this research work, we have analysis and compared the various biometric authentications in which DNA is better in context of various factors as shown in 2. Retina, Heart beat and Iris plays very important role to identification of authorized person. Finally these systems are highly confidential, secured and accurate compare to all other traditional authentication system.

vides protection, privacy from fraud. In this research work, we have analysis and compared the various biometric authentications in which DNA is better in context of various factors as shown in 2. Retina, Heart beat and Iris plays very important role to identification of authorized person. Finally these systems are highly confidential, secured and accurate compare to all other traditional authentication system.

### REFERENCES

1. D. Bhattacharya, R. Ranjan, F. Alisherov, and C. Minkyu., Biometric Authentication: A Review, International Journal of u-and e-Service, Science and Technology IJUES, Vol. 2(3), pp.13-28, 2009.
2. S. Singh , A Review on Biometrics and Ear Recognition Technique, IJARCSSE, Vol. 3(6), pp.1624-1630, 2009.
3. S. R. Kodituwakku, Biometric Authentication: A Review, International Journal of Trend in Research and Development, Vol. 2(4), pp.2394-9333, 2015.
4. S. Gaur, V. A. Shah and M. Thakker, Biometric Recognition Techniques: A Review, IJAREIE, Vol. 1(4), pp.282-290, 2012.
5. H. Srivastava., A Comparison Based Study on Biometrics for Human Recognition, IOSR-JCE, Vol. 15(1), pp.22-29, 2013.
6. S. Tiwari, J.N. Chaurasia and V.S Chaurasia, A Review of Advancements in Biometric Systems, IJIRAE, Vol. 2(1), pp. 187-204, 2015.
7. B. Kaschte, Biometric Authentication System Today and In The Future, IEEE, Vol. 2(4), pp. 1-13, 2005.

8. A.K. Jain, A. Ross and S. R. Prabhakar, An Introduction to Biometric Recognition, IEEE, Vol. 14(1), pp. 1-29, 2004.
9. BTAM, Biometric Technology Application Manual: Applying Biometrics, National Biometric Security Project, Vol. 2, pp. 3-176, 2008.
10. R. Saini and N. Rana, Comparison of Various Biometric Method, IJAST, Vol. 2(1), pp.24-30, 2014.
11. Website[<http://lonewlf176.blogspot.in/2010/10/facial-recognition-advantages-and.html>] [Browsing date:23-02-2017].
12. Weblink[<http://www.cl.cam.ac.uk/~jgd1000/addisadvans.html>][Browsing date: 30/02/2017].
13. Weblink[[http://www.globalsecurity.org/security/systems/biometricseye\\_scan.htm](http://www.globalsecurity.org/security/systems/biometricseye_scan.htm)][Browsing date :20/04/2017].
14. Website [<http://resources.infosecinstitute.com>] [Browsing date: 03-01-2017].
15. Weblink[<http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies>] [Browsing date: 07-01-2017].
16. I. M. Alsaadi, Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH Vol. 4(12), pp.285-289, 2015.
17. A. Babich, Biometric authentication Types of biometric identifiers, Bachelor's Thesis, Haaga-Helia University of applied science, 2012.
18. M. M. Sawant, Y. Nagargoje., S. Selki, D. Bora and Y. Borate, Keystroke Dynamics: Review Paper, IJARCCCE, 2(10)4018-4020, 2013.
19. Weblink[<http://www.ijstr.org/final-print/dec2015/Physiological-Biometric-Authentication-Systems-Advantages-Disadvantages-And-Future-Development-A-Review.pdf>][Browsing date:22/03/2017].